ATIS STANDARD

# ATIS-0800024

# SECURITY ROBUSTNESS RULES INTEROPERABILITY SPECIFICATION

The Alliance for Telecommunication Industry Solutions (ATIS) is a technical planning and standards development organization that is committed to rapidly developing and promoting technical and operations standards for the communications and related information technologies industry worldwide using a pragmatic, flexible and open approach. Over 1,100 participants from over 300 communications companies are active in ATIS' 22 industry committees and its Incubator Solutions Program.

**< http://www.atis.org/ >**


**Notice of Disclaimer & Limitation of Liability**

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER, NO REPRESENTATION OR WARRANTY IS MADE OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. ATIS SHALL NOT BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY ATIS FOR THIS DOCUMENT, WITH RESPECT TO ANY CLAIM, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES ANY AND ALL USE OF OR RELIANCE UPON THIS INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

NOTE - The user's attention is called to the possibility that compliance with this standard may require use of an invention covered by patent rights. By publication of this standard, no position is taken with respect to whether use of an invention covered by patent rights will be required, and if any such use is required no position is taken regarding the validity of this claim or any patent rights in connection therewith.


ATIS-0800024, *Security Robustness Rules Interoperability Specification*

Is an ATIS standard developed by the **IPTV Security Solutions (ISS)** Committee under the **ATIS IPTV Interoperability Forum (IIF)**.


*Published by*

**Alliance for Telecommunications Industry Solutions**
**1200 G Street, NW, Suite 500**
**Washington, DC 20005**



Copyright © 2008 by Alliance for Telecommunications Industry Solutions
All rights reserved.

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher. For information contact ATIS at 202.628.6380. ATIS is online at < http://www.atis.org >.



Printed in the United States of America.

**ATIS-0800024**

ATIS Standard

# SECURITY ROBUSTNESS RULES INTEROPERABILITY SPECIFICATION

**Alliance for Telecommunications Industry Solutions**

Approved March 17, 2009

**Abstract**

In the interest of promoting and maintaining secure environments for handling, storing, and transmitting of sensitive material, such as keys, certificates, operating code, etc., this document defines the IPTV interoperability specifications for Security Robustness Rules. This specification pertains to IPTV devices both on the server side and on the receiving side. This document augments the IPTV Security Solutions (ISS) Security Profiles by defining Secure Execution Environment elements and their robustness levels. The ISS Security Profiles and robustness levels may be useful in matching content value to platform security capability.

## FOREWORD

The Alliance for Telecommunication Industry Solutions (ATIS) serves the public through improved understanding between carriers, customers, and manufacturers. The IPTV Interoperability Forum (IIF) develops requirements, standards, and specifications that will determine the industry's end-to-end solution for Internet Protocol Television (IPTV).

The mandatory requirements are designated by the word *shall* and recommendations by the word *should*. Where both a mandatory requirement and a recommendation are specified for the same criterion, the recommendation represents a goal currently identifiable as having distinct compatibility or performance advantages.

Suggestions for improvement of this document are welcome. They should be sent to the Alliance for Telecommunications Industry Solutions, IIF Staff, 1200 G Street NW, Suite 500, Washington, DC 20005.

The IPTV Security Solutions (ISS) Committee was responsible for the development of this document, with the leadership of the following people:

D. O'Callaghan, IIF Chair
R. Brand, IIF Vice Chair
M. Nakhjiri, ISS Committee Co-Chair
T. Wasilewski, ISS Committee Co-Chair
C.A. Underkoffler, ATIS Chief Editor
A. Blasgen, IIF Committee Administrator
B. Scarpelli, IIF Committee Administrator

## CONTRIBUTORS

Phyllis Anderson, AT&T
Cristina Serban, AT&T
David Sedacca, Cisco
Tony Wasilewski, Cisco
Mark Murray, Cisco
Madjid Nakhjiri, Motorola
Niranjan Samant, Motorola
Robin Wilson, Nagravision
Steve White, Nagravision
Hasler Hayes, Nortel
Jean-Yves Bernard, Rogers Communications
Neerav Shah, Verimatrix

## TABLE OF CONTENTS

**1 INTRODUCTION ..... 1**

1.1 OBJECTIVE ..... 1
1.2 OVERVIEW ..... 1
1.3 SECURITY ROBUSTNESS ..... 3
1.4 SECURE EXECUTION ENVIRONMENT ..... 3

**2 NORMATIVE REFERENCES ..... 3**

**3 DEFINITIONS, ACRONYMS, & ABBREVIATIONS ..... 4**

3.1 DEFINITIONS ..... 4
3.2 ACRONYMS & ABBREVIATIONS ..... 6

**4 ANALYSIS FOR INTEROPERABILITY ..... 7**

4.1 USE CASES ..... 7
*4.1.1 Protection of Content While In Motion or At Rest ..... 7*
*4.1.2 Analog Copy Protection Requirements ..... 7*
*4.1.3 Digital Copy Protection Requirements ..... 7*
*4.1.4 Impact of Robustness Rules on Subscribers ..... 8*
4.2 IPTV SYSTEMS – THREAT ANALYSIS ..... 8
4.3 THREATS TO IPTV DEVICES ..... 17
*4.3.1 Threats to Outputs and Paths ..... 17*
*4.3.2 Device Information Integrity ..... 17*
4.4 GENERAL SCOPE OF ROBUSTNESS RULES ..... 18

**5 DESIGN FOR INTEROPERABILITY ..... 18**

5.1 SECURE EXECUTION ENVIRONMENT ELEMENTS ..... 18
*5.1.1 Execution Engine ..... 18*
*5.1.2 Storage ..... 18*
*5.1.3 Trusted Paths ..... 19*
*5.1.4 Physical Security ..... 19*
*5.1.5 Algorithms ..... 19*
*5.1.6 Secure Time Generation ..... 19*
5.2 ROBUSTNESS LEVELS ..... 19
*5.2.1 No Element Robustness ..... 19*
*5.2.2 Low Element Robustness ..... 20*
*5.2.3 High Element Robustness ..... 20*
5.3 SECURE EXECUTION ENVIRONMENT LEVELS ..... 20
5.4 ROBUSTNESS RULES TO FIPS 140-2 MAPPING ..... 21
5.5 CONFIDENTIALITY AND INTEGRITY PROTECTION ..... 23
5.6 RELATIONSHIP TO ISS SECURITY PROFILES ..... 23
*5.6.1 ISS Profile Level 0 ..... 23*
*5.6.2 ISS Profile Level 1 ..... 23*
*5.6.3 ISS Profile Level 2 ..... 24*
*5.6.4 ISS Profile Level 3 ..... 24*
*5.6.5 ISS Profile Level 4 ..... 24*

**6 REQUIREMENTS TO SPECIFICATION MAPPING ..... 25**

**ANNEX A (INFORMATIVE) ..... 26**

A.1 REQUIREMENTS LABELING GUIDELINE ..... 26

## TABLE OF FIGURES

FIGURE 1: INTER-RELATIONSHIP OF IIF ISS SPECIFICATIONS ..... 2
FIGURE 2: IPTV SYSTEM THREATS ..... 9
FIGURE 3: IPTV RECEIVING DEVICE – CONTENT THEFT - CONTENT SPLICING - ATTACK TREE ..... 9
FIGURE 4: IPTV RECEIVING DEVICE –CONTENT THEFT - CAPTURE CLEAR CONTENT – ATTACK TREE ..... 10
FIGURE 5: IPTV RECEIVING DEVICE- CONTENT THEFT - DECRYPTED ENCRYPTED CONTENT - ATTACK TREE ..... 11
FIGURE 6: IPTV RECEIVING DEVICE CONTENT THEFT - DUPLICATE DEVICE WITH KEY INFORMATION - ATTACK TREE ..... 12

FIGURE 7: IPTV RECEIVING DEVICE CONTENT THEFT – USE OF REVOKED CERTIFICATE - ATTACK TREE ..... 12
FIGURE 8: IPTV RECEIVING DEVICE - SERVICE THEFT - ATTACK TREE ..... 13
FIGURE 9: IPTV RECEIVING DEVICE - SERVICE THEFT - MANIPULATE EMMS - ATTACK TREE ..... 14
FIGURE 10: IPTV RECEIVING DEVICE - SERVICE THEFT - IGNORE EMM REMOVAL - ATTACK TREE ..... 15
FIGURE 11: IPTV RECEIVING DEVICE - SERVICE THEFT - DUPLICATE DEVICE - ATTACK TREE ..... 15
FIGURE 12: IPTV RECEIVING DEVICE - INFORMATION THEFT - ATTACK TREE ..... 16
FIGURE 13: IPTV RECEIVING DEVICE - SERVICE DISRUPTION - ATTACK TREE ..... 17

## TABLE OF TABLES

TABLE 1: SECURE EXECUTION ENVIRONMENT LEVELS ..... 20
TABLE 2: ROBUSTNESS RULES TO FIPS 140-2 MAPPING ..... 22
TABLE 3: CONFIDENTIALITY AND INTEGRITY PROTECTION ..... 23
TABLE 4: SEE SUB-PROFILES OF ISS PROFILE LEVEL 3 ..... 24
TABLE 5: SEE SUB-PROFILES OF ISS PROFILE LEVEL 4 ..... 24

ATIS Standard on –

# Security Robustness Rules Interoperability Specification

## 1 INTRODUCTION

### 1.1 Objective

As part of its technical framework, the ATIS IIF has defined the concepts of IPTV Security Solution (ISS), Native Security Solution (NSS), and ISS Security Profiles. Specifically in ATIS-0800014 [1], ISS Security Profiles provide a characterization of the security environment of the IPTV devices with respect to the type of NSS and the existence of a Secure Execution Environment (SEE). While NSS is comprised of the hardware and software present at the manufacturing time with the intent to provide an SEE, the exact implementation of the NSS may differ for each manufacturer. Within ATIS-0800014, the definition and requirements for the SEE is considered to be part of the definition of robustness rules.

The term *robustness rules* typically refers to technical as well as business and legal requirements that a device manufacturer must fulfill within a licensing framework. However, the business and legal requirements pertaining to robustness rules are outside the scope of this technical specification.

As a general principle, ATIS IIF specifications consider the Digital Rights Management (DRM) Component to be a black box.

The scope of this specification includes a set of robustness rules for IPTV devices. These rules are intended to enable functions such as content protection, secure control messaging and consumer privacy. This document, *Security Robustness Rules Interoperability Specification*, meets the following objectives:

1. To focus on interoperability solutions only.
2. To specify the security robustness rules of the IPTV Devices, including IPTV Receiving Devices and IPTV server-side devices and equipment.
3. To define the requirements for a SEE. This includes the following SEE elements: execution engine, storage, trusted paths, physical security, algorithms, and secure time generation.
4. To map the security robustness rules of this document to components of FIPS 140-2.
5. To define the link between robustness rules for SEE and the ISS Security Profiles.

### 1.2 Overview

This document refers to the overall security solutions context and architecture discussed in ATIS-0800001 [5].

The following figure highlights the inter-relationship of many of the ATIS IIF specifications.

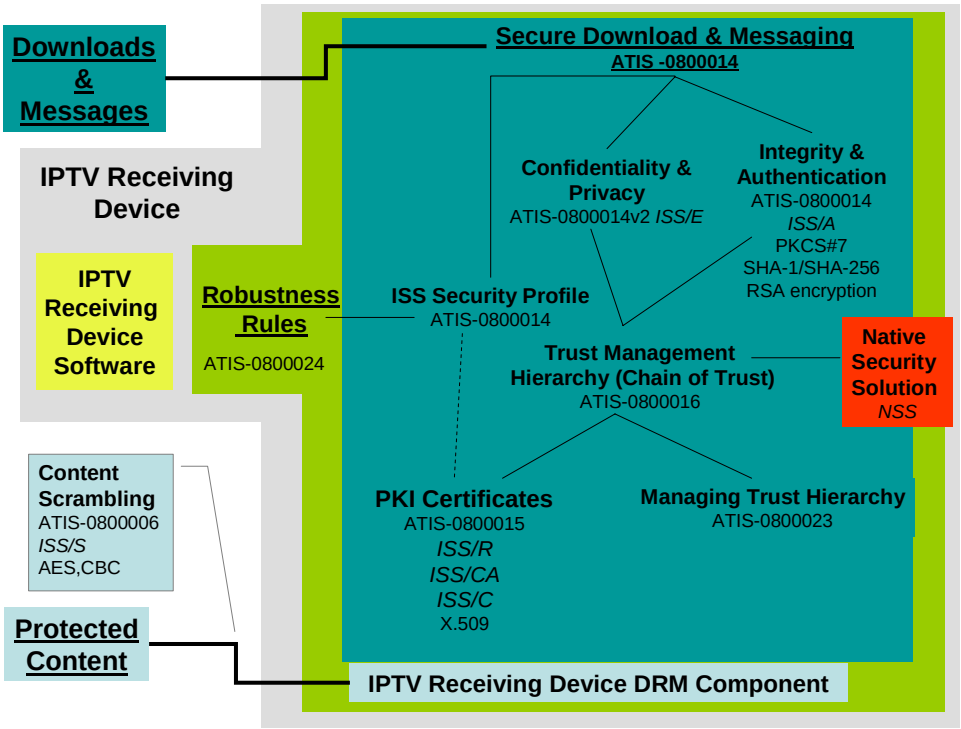


**Figure 1: Inter-Relationship of IIF ISS Specifications**

Protected Content that flows to any IPTV Receiving Device DRM Component is protected while in transit using content scrambling (ISS/S) following the method outlined in ATIS-0800006 [2]. The method is based upon the widely recognized 128-bit AES CBC method. The protected content is terminated within the IPTV Receiving Device DRM Component.

Secure downloads and secure messaging to the IPTV Devices is defined in ATIS-0800014 [1]. The widely recognized PKCS#7 method is used as the basis for ISS/A, the authentication functionality, and utilizes public key certificates organized into a trust hierarchy as described in ATIS-0800015 [3]. Version 2 of ATIS-0800014 will, by the specification of an encryption functionality (ISS/E), enable confidentially and privacy of messages and secure downloads (not protected content) destined to any IPTV Devices.

ATIS-0800014 also specifies how the authentication functionality and the security characteristics of the execution environment form a range of ISS Security Profiles. ISS Security Profiles are intended to support commercial decisions regarding what content will be made available to IPTV Devices. The ISS Security Profiles defined in ATIS-0800014 also introduce the concept of a Secure Execution Environment (SEE). The robustness definitions in this document determine whether a SEE exists or not, and if one does, defines the robustness level of that SEE.

Manufacturers of IPTV Devices may provide a Native Security Solution (NSS) in order to help secure a Chain of Trust. An NSS (discussed in ATIS-0800014) is composed of hardware and/or software elements chosen by the manufacturer that are implemented at manufacturing time.

ITU-T X.509 is used as the basic format for various types of certificates, as defined in ATIS-0800016 [4]. Some of these certificates may reside within IPTV Devices (e.g., ISS/C). Other types of certificates are defined for use by certificate authorities (ISS/CA) and for use by root authorities (ISS/R).

ATIS-0800023, *Managing the IIF Trust Hierarchy Interoperability Specification*, outlines how these certificates and the associated trust hierarchy are managed during their entire lifecycle.

This document defines the factors required to achieve an appropriately secure and robust environment and relates these factors to the ISS Security Profiles outlined in ATIS-0800014.

### 1.3 Security Robustness

*Security Robustness* refers to the logical and physical means employed in manufactured devices to thwart attempts to modify, compromise, and/or exert unauthorized control over these devices. The intended effect of these attempts can include, for example, defeating content protection mechanisms, compromising sensitive information, producing illegitimate replicas of IPTV devices, and violating service level agreements.

### 1.4 Secure Execution Environment

The Secure Execution Environment (SEE) is a combination of hardware and software components inside a device as well as interfaces between those components that prevent attackers from stealing cryptographic keying material, protected content, or any other protected information from the device. SEEs have to withstand various levels of attack sophistication, ranging from hobbyists with commonly available tools to well-funded adversaries with strong engineering backgrounds and leading-edge tools. This document defines a set of SEE levels that characterize the level of resistance to these attacks.

## 2 NORMATIVE REFERENCES

The following standards contain provisions which, through reference in this text, constitute provisions of this ATIS Standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this ATIS Standard are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below.

[1] ATIS-0800014, *Secure Download and Messaging Interoperability Specification*, March 2008. [1]

[2] ATIS-0800006, *IIF Default Scrambling Algorithm (IDSA) IPTV Interoperability Specification*, January 2007.[1]

[3] ATIS-0800015, *Certificate Trust Management Hierarchy Interoperability Specification*, August 2008. [1]

[4] ATIS-0800016, *Standard PKI Certificate Format Interoperability Specification*, August 2008. [1]

[5] ATIS-0800001, *IPTV DRM Interoperability Requirements*, May 2007. [1]

[6] ATIS-0800023, *Managing the IIF Trust Hierarchy Interoperability Specification*, to be published. [1]

[7] FIPS PUB 140-2, *Security Requirements for Cryptographic Modules*, May 2001.[2]

[1] This document is available from the Alliance for Telecommunications Industry Solutions, 1200 G Street N.W., Suite 500, Washington, DC 20005. <http://www.atis.org>

[2] This document is available from the National Institute of Standards and Technology (NIST). < http://www.nist.gov/ >

# 3 DEFINITIONS, ACRONYMS, & ABBREVIATIONS

## 3.1 Definitions

**3.1.1 Access Control:** The practice of restricting the viewing of TV or the interaction with IPTV applications to authorized persons and to the mechanisms which prevent access by unauthorized persons. It includes:

- Control of boot-load and application load onto the IPTV Receiving Device.
- Control of access to the service and to the IPTV Receiving Device.
- Protection of the data carried between IPTV Receiving Device and Service Provider.
- Authentication between user or IPTV Receiving Device and Service Provider.

**3.1.2 Authentication**: A mechanism that allows verifying an entity's identity in order to ensure that they are who they claim to be.

**3.1.2 Authorization:** A mechanism that defines and controls what services or resources an entity can access.

**3.1.2 Black Box:** A component whose internal structure and operations are not specified.

**3.1.3 Certificate:** Information that binds a public key to the distinguished name of the owner/user of the public key in an authorized manner.

**3.1.4 Certificate Authority:** An organization that issues certificates that are recognized by other parties as being trusted.

**3.1.5 Conditional Access System**: A mechanism that is used to protect and control the viewing of traditional broadcast TV content, on-demand content, and pay-per-view. It has been implemented over uni-directional and bi-directional networks and co-channel transport. It is used both in analog TV broadcast systems and in digital TV delivery systems (where the equivalent of analog de-scrambling for digital services is implemented).

NOTE – The ATIS IIF agrees that there is not a hard split between Conditional Access and DRM, and as functionalities are added to Conditional Access, the difference narrows.

**3.1.6 Confidentiality:** The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

**3.1.7 Content:** One or more *Media Objects*.

**3.1.8 Content Issuer:** The entity that makes content available; the entity whose *Content* is being Protected.

**3.1.9 Content Protection:** A combination of *Access Control* and *Copy Control*.

**3.1.10 Content Provider:** An entity that is either a *Content Issuer* or a *Rights Issuer*.

**3.1.11 Content Subscription:** A subscription that a *User* has with a *Content Provider* for the purposes of paying for *Protected Content* purchased from that Content Provider and played on a User's *Device*.

**3.1.12 Copy:** To make a perfect reproduction of *DRM Content* or *Rights*.

**3.1.13 Copy Control:** The enforcement of conditions under which copyrighted content can be copied. Copy Control is one part of *Content Protection*.

**3.1.14 Copy Protection:** A mechanism used to protect content from being copied in an unauthorized manner via analog and/or digital *IPTV Receiving Device* interfaces. Copy Protection is a combination of *Access Control* and *Copy Control*.

**3.1.15 Cryptographically Robust:** This term *cryptographically robust* is often used to describe an encryption algorithm and implies, in comparison to some other algorithm (which is thus cryptographically weaker), greater resistance to attack.

**3.1.16 Device:** A Device is the entity (hardware/software or combination thereof) within a user's equipment that implements a *DRM Client*. The Device is also conformant to the specifications of the DRM it supports.

**3.1.17 DRM:** A collection of technologies that technically enable the definition of and the enforcement of secure content transportation as well as secure content licensing, including:

- Protection and control of the viewing of content that is delivered over IP transport.
- Rights Management for the delivered content.

**3.1.18 DRM Client:** The entity in the *Device* that manages *Permissions* for *Content* and *Media Objects* on the *Device*.

**3.1.19 Entitlement:** Information about the authorization level/s a user has to access and use certain services and to access, use, copy, and distribute certain contents received in his/her *IPTV Receiving Device*.

**3.1.20 Integrity:** The property that data (*Contents*, *Rights*, etc.) has not been altered or destroyed in an unauthorized manner.

**3.1.21 IPTV Device:** *IPTV Receiving Device* or server-side devices or equipment.

**3.1.22 IPTV Receiving Device:** IPTV Terminal Function (ITF) and Delivery Network Gateway (DNG) as defined in ATIS-0800002, *IPTV Architecture Requirements*, represents the functionality within the consumer network that is responsible for terminating the IP signal and converting the content into a renderable format (e.g., a STB).

**3.1.23 ISS/A:** The part of the ISS toolkit that deals with authentication functionality. See ATIS-0800014, *Secure Download and Messaging Interoperability Specification*.

**3.1.24 ISS/E:** The part of the ISS toolkit that deals with confidentiality functionality. See ATIS-0800014, *Secure Download and Messaging Interoperability Specification*.

**3.1.25 ISS/S:** The part of the ISS toolkit that deals with content scrambling. See ATIS-0800006, *IIF Default Scrambling Algorithm*.

**3.1.26 Key Management:** All of the provisions made in a secure IPTV system, which are related to the generation, transport, exchange, storage, safeguarding, use, revocation, and renewing of cryptographic keys.

**3.1.27 Message Integrity:** The quality of a transmitted message, such that its recipient can be assured that the contents of the message have not been tampered with or altered since the time it was transmitted by the sender. One common approach is to use a one-way hash function that combines all of the bytes in the message to produce a message digest that is impossible to reverse, and then make a digital signature of this hash value by the sender. Another method involves combining message bytes with a key value known only to the sender and recipient in a hash function.

**3.1.28 Native Security Solution:** The hardware and software present at manufacturing time, designed to secure the execution environment of an *IPTV Receiving Device*.

**3.1.29 Privacy:** Confidentiality of user viewership and interactions with IPTV systems.

**3.1.30 Protected Content:** *Media Objects* that are consumed according to a set of *Permissions* in a *Rights Object*.

**3.1.31 Revoke:** A *Device* has been Revoked by a particular *Rights Issuer* if that Rights Issuer has decided it does not wish to issue *Rights Objects* to that Device (for example, because it has concerns about the robustness of the Device's implementation).

**3.1.32 Rights:** The ability to perform a pre-defined set of utilization functions on a content item. These utilization functions are the permissions (e.g., to view/hear, copy, modify, record, excerpt, sample, translate in another language, keep for a certain period, distribute), constraints (e.g., play/view/hear multiple times, play/view/hear certain number of hours), and obligations (e.g., payment, tracking information) that apply to the content and provide liberty of use granted to the end-user.

**3.1.33 Rights Expression:** The statement of utilization functions that can be performed on a *Content Item* and the conditions in which they can be performed.

**3.1.34 Rights Holder:** Indicates the entity that is entitled to grant rights.

**3.1.35 Separable Security Element:** The module providing operator based conditional access, which is not an integral part of the *IPTV Receiving Device* at manufacture time.

**3.1.36 Server-Side Middleware:** This is the system external to the Server-Side DRM System that is interacting with the Server-Side *DRM System* to facilitate the delivery of secure content to the *IPTV Receiving Device*.

## 3.2 Acronyms & Abbreviations

| | |
|---|---|
| AES | Advanced Encryption Standard |
| ATIS | Alliance for Telecommunications Industry Solutions |
| CA | Certificate Authority |
| CAS | Conditional Access System |
| CBC | Cipher Block Chaining |
| DRM | Digital Rights Management |
| DVB | Digital Video Broadcasting |
| FIPS | Federal Information Processing Standard |
| IDSA | IIF Default Scrambling Algorithm |
| IPTV | Internet Protocol Television |
| IETF | Internet Engineering Task Force |
| IIF | IPTV Interoperability Forum |
| IP | Internet Protocol |
| ISO | International Organization for Standardization |
| ISS | IPTV Security Solution |
| ISS/A | IPTV Security Solution/Authentication |
| ISS/C | IPTV Security Solution/Certificate |
| ISS/CA | IPTV Security Solution/Certificate Authority |
| ISS/E | IPTV Security Solution/Encryption |
| ISS/R | IPTV Security Solution/Root |
| ISS/S | IPTV Security Solution/Scrambling |
| ITF | IPTV Terminal Function |
| NIST | National Institute of Standards and Technology |
| NSS | Native Security Solution |
| OI | Object Identifier |

| | |
|---|---|
| OU | Organizational Unit |
| PKCS | Public Key Cryptography Standards |
| SEE | Secure Execution Environment |
| SSE | Separable Security Element |
| URI | Uniform Resource Identifier |

# 4 ANALYSIS FOR INTEROPERABILITY

## 4.1 Use Cases

The following use cases are relevant in the analysis leading to the specification of the robustness rules.

### 4.1.1 Protection of Content While In Motion or At Rest

Content that needs to be protected from illegitimate interception needs to be transported in an encrypted format where the encryption/decryption keys are only made available to authorized users. A SEE can contribute to enhanced security for key storage and key usage.

Similarly, the need to keep stored content in a protected state is important and can also be achieved through suitable encryption methods.

The above considerations suggest that:

- Protected content *should not* be stored in the clear. Cryptographic keys related to security of content (e.g., content decryption keys) *should* also be protected while in storage or in use.
- Protected content *should not* be transferred to any other device in the clear. Cryptographic keys related to security of content *should not* be transferred to other devices in the clear.

### 4.1.2 Analog Copy Protection Requirements

Real world content delivery systems have requirements for analog copy protection. Some examples of well known analog signal copy protection systems are:

- CGMS-A
  - NTSC:
    - Line 20 (IEC 61880)
    - Line 21 XDS (EIA/CEA 608)
  - CEA 805
- Macrovision's ACP

The execution of analog copy protection mechanisms on IPTV Receiving Devices can benefit from secure operating conditions.

### 4.1.3 Digital Copy Protection Requirements

Real world content delivery systems have requirements for digital copy protection. Some examples of well known digital signal copy protection systems are:

- DTCP

- HDCP

The execution of digital copy protection mechanisms on IPTV Receiving Devices can benefit from secure operating conditions.

#### 4.1.4 Impact of Robustness Rules on Subscribers

The following use case highlights how Robustness Rules impact the interoperability of IPTV from the subscriber's view point. When subscribers choose to purchase a receiving device product, they must take into consideration the security robustness requirements for the content they intend to consume. For example, a subscriber could acquire devices of different ISS Security Profiles and SEE robustness levels, some of which may not be permitted to receive high-value content or replay content that was previously stored on other receiving devices in the subscriber's domain. For example, a content owner has decided to allow:

- Premium content to be playable only on IPTV Receiving Devices that meet ISS Profile 3 or 4.
- Non-premium content to be playable on IPTV Receiving Devices that meet ISS Profile 2, 3, or 4.

Therefore, if a given subscriber desires to receive premium content from this content owner, this subscriber will need to use a device which meets ISS Security Profiles 3 or 4.

While this subscriber need not be aware of the specific characteristics of the IPTV Robustness Rules, the ISS Security Profile and SEE robustness mechanisms present an easy-to-understand identification of device capabilities for content reception. For example, ISS Security Profiles could be used as part of a labeling or branding scheme for IPTV interoperability. However, such a branding or labeling method is outside of the scope of this document.

### *4.2 IPTV Systems – Threat Analysis*

This section provides a non-exhaustive threat analysis for an IPTV system, including IPTV service (content delivery) from IPTV server side components to IPTV Receiving Devices, and content storage in and output from IPTV Receiving Devices. The threats presented here may require various forms of mitigations. Complying with the device robustness requirements described in this document would possibly mitigate only a sub-set of these threats, and thus would need to be supplemented by other mitigation techniques not covered in this document. For example, such additional techniques include mechanisms described in other ATIS documents, such as the ATIS-08000006, *IIF Default Scrambling Algorithm,* or certificate management mechanisms for trust establishment.

In the figures of this section, potential vulnerabilities are shown within boxes while possible mitigations are shown within ovals. The mitigation strategies described for a single threat may need to be applied collectively rather than as alternatives. Furthermore, the mitigations noted in this section do not represent a complete list and thus may not provide full protection against the mentioned threats.

#### 4.2.1 IPTV System Threats

Each of the four threats shown in the next figure is decomposed into more detail in the following subsections.

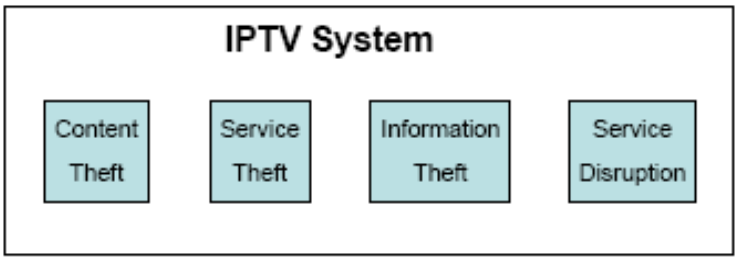


**Figure 2: IPTV System Threats**

#### 4.2.1.1 Content Theft

*Content theft* involves the acquiring of protected content which can then be freely copied or distributed by the attacker. The next figure shows the attack tree for content theft by *content splicing*. This threat has two potential branches – either the would-be attacker has access to multiple streams of the same content and/or the attacker will need to extrapolate over any partially encrypted content. The mitigation strategy for content theft through content splicing is to fully encrypt the content instead of using partial encryption.

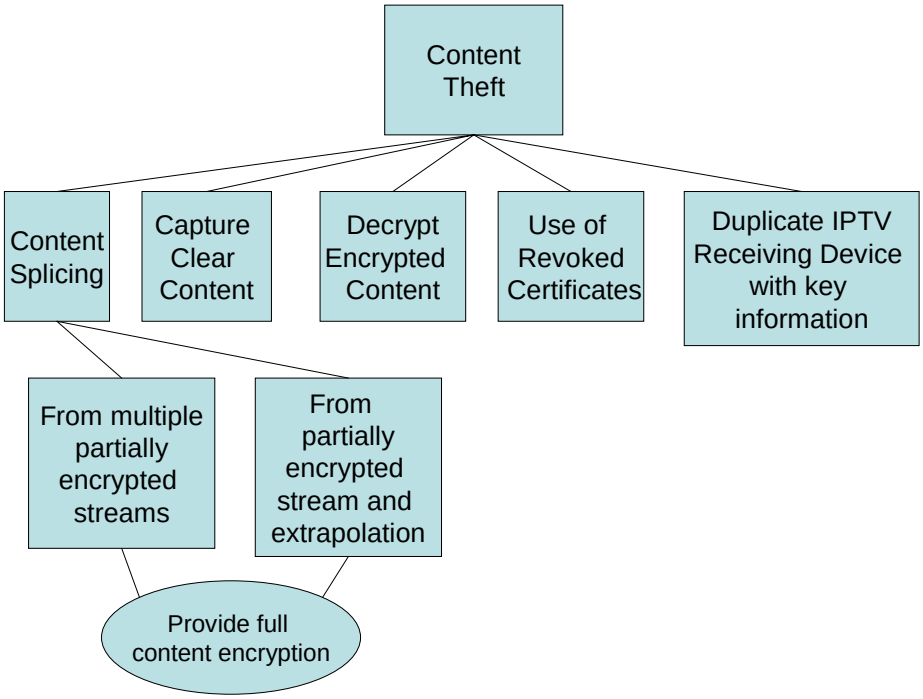


**Figure 3: IPTV Receiving Device – Content Theft - Content Splicing - Attack Tree**

The next figure shows the attack tree for content theft by *capture clear content*. This vulnerability has two potential branches dependent upon whether or not the IPTV Receiving Device has either analog and digital signals, or both. These signals could be either external to or within the IPTV Receiving Device. After the content that requires protection has been delivered to the device through the broadcast or

multicast service, it *should* be afforded content protection mechanisms while in storage or during transfer to other devices or while being rendered. Content that requires protection *should not* be stored in the clear.

High value content *should not* allow analog output as analog outputs are more difficult to protect.

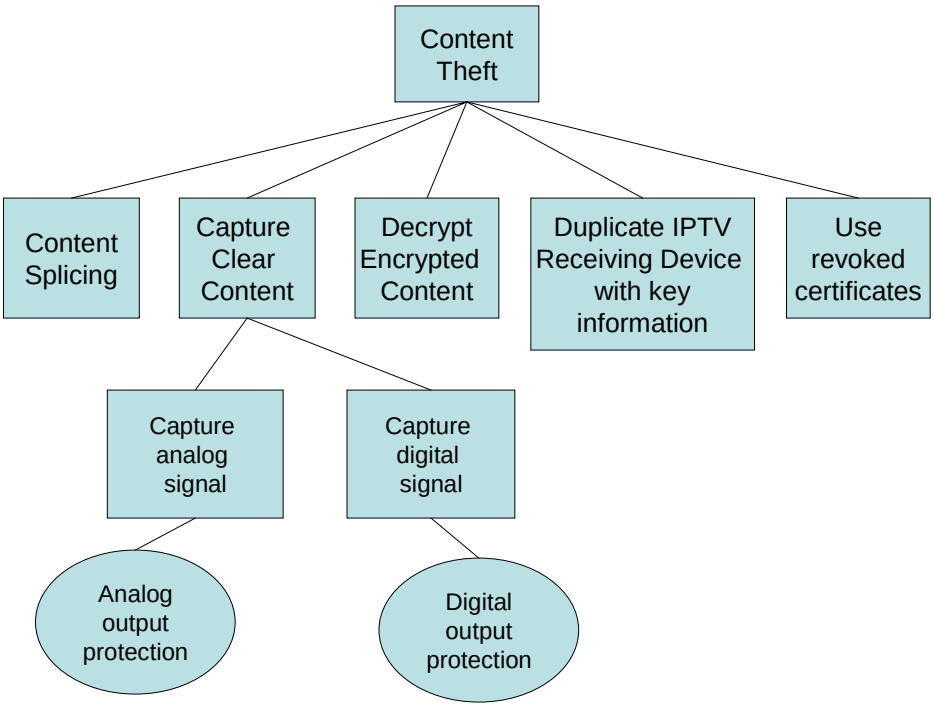


**Figure 4: IPTV Receiving Device –Content Theft - Capture Clear Content – Attack Tree**

The next figure shows the attack tree for content theft by *decrypt encrypted content*. This has two branches - capturing encrypted content and/or stealing the keys for the encrypted content.

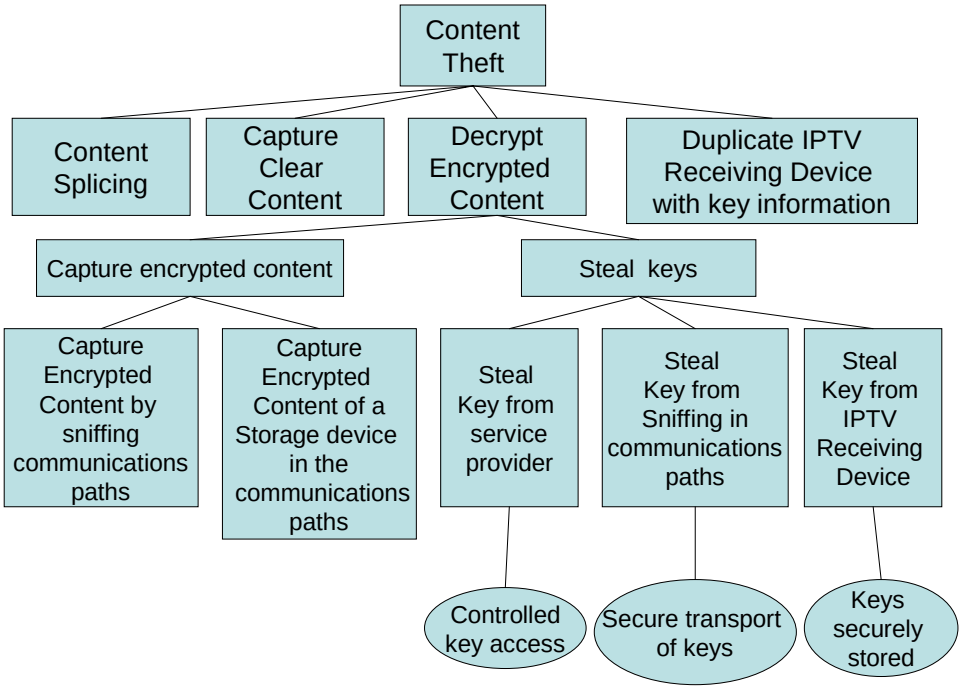


**Figure 5: IPTV Receiving Device- Content Theft - Decrypted Encrypted Content - Attack Tree**

In the above figure, securing keys means that: 1) keys cannot be directly read or copied by those processes not authorized to do so; and 2) keys cannot be directly read by hardware means. Part of the mitigation strategy of this vulnerability is complying with the robustness rules described in this document.

The next figure shows the attack tree for content theft by impersonating a valid IPTV Receiving Device.

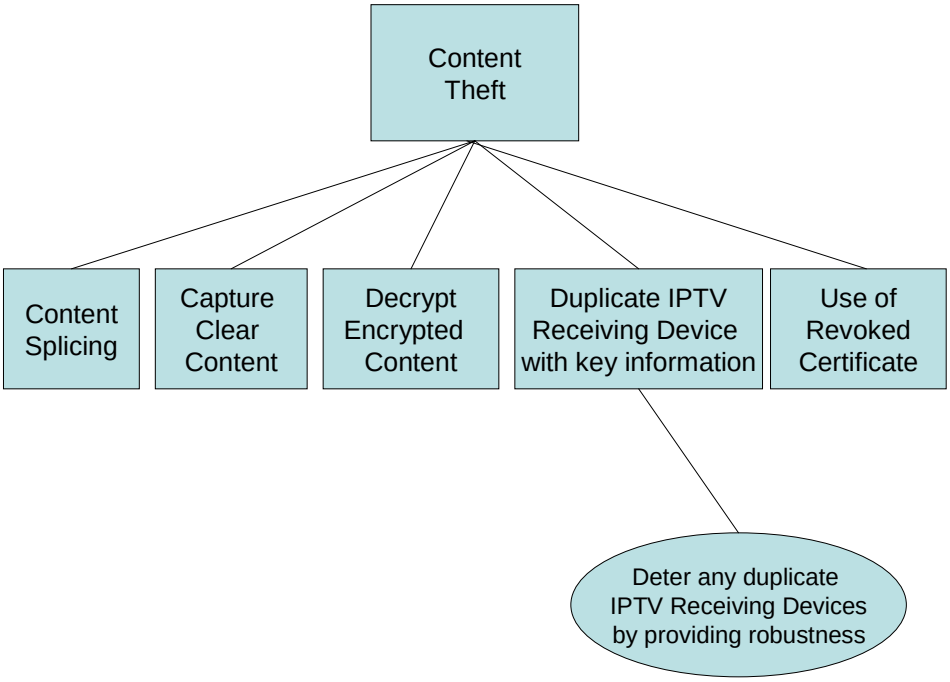


**Figure 6: IPTV Receiving Device Content Theft - Duplicate Device with key information - Attack Tree**

Part of the mitigation strategy of this vulnerability may also involve various levels of tamper proofing.

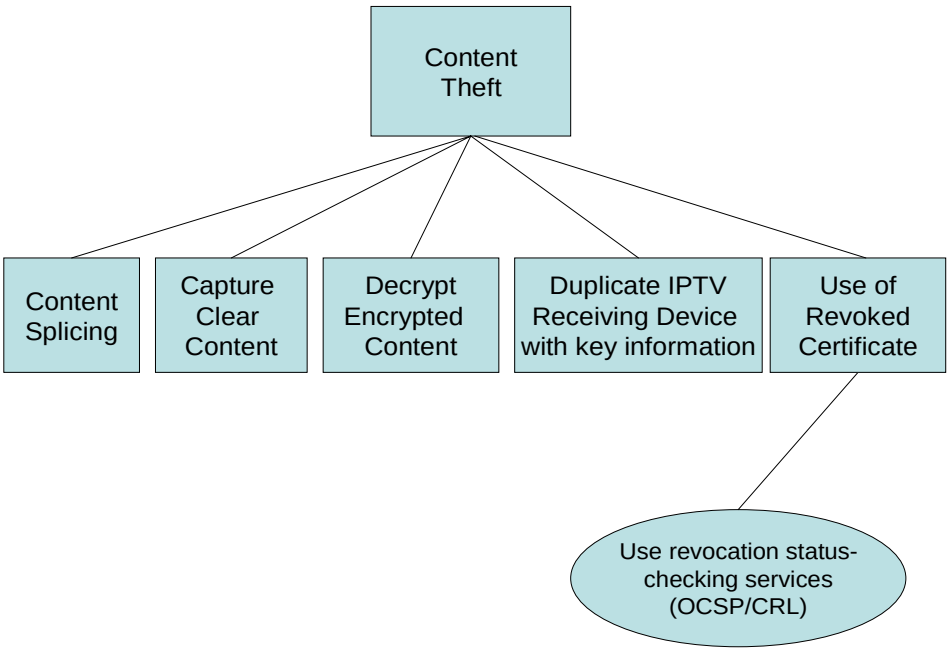


**Figure 7: IPTV Receiving Device Content Theft – Use of Revoked Certificate - Attack Tree**

#### 4.2.1.2 Service Theft

*Service theft* involves the viewing of video content which the attacker has not paid for; the next figure shows this attack tree. This service theft vulnerability has three attack branches that are decomposed in further figures:

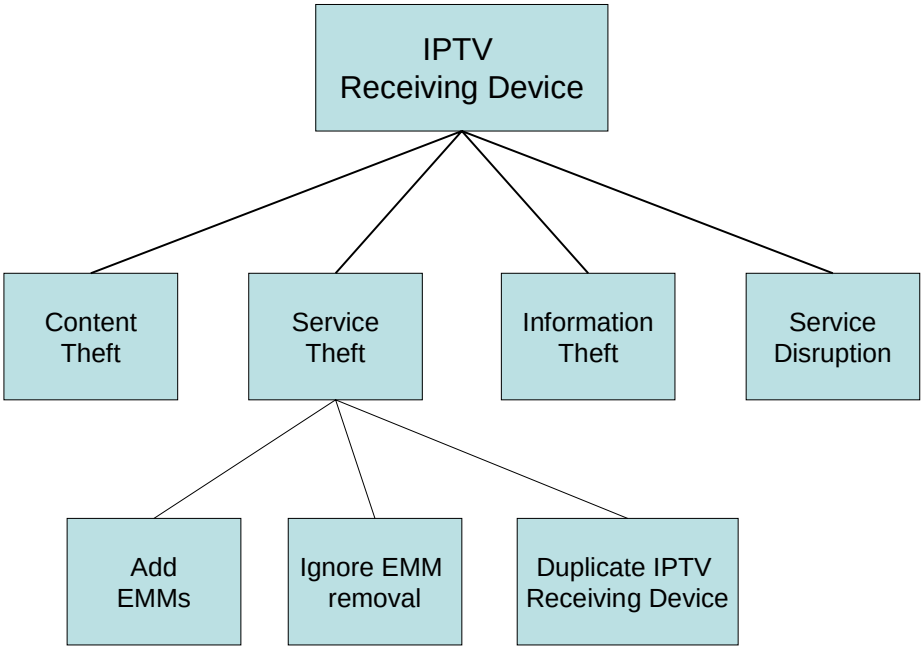


**Figure 8: IPTV Receiving Device - Service Theft - Attack Tree**

The next figure shows the attack tree for service theft by manipulating EMMs. This attack tree has three more sub-branches as shown:

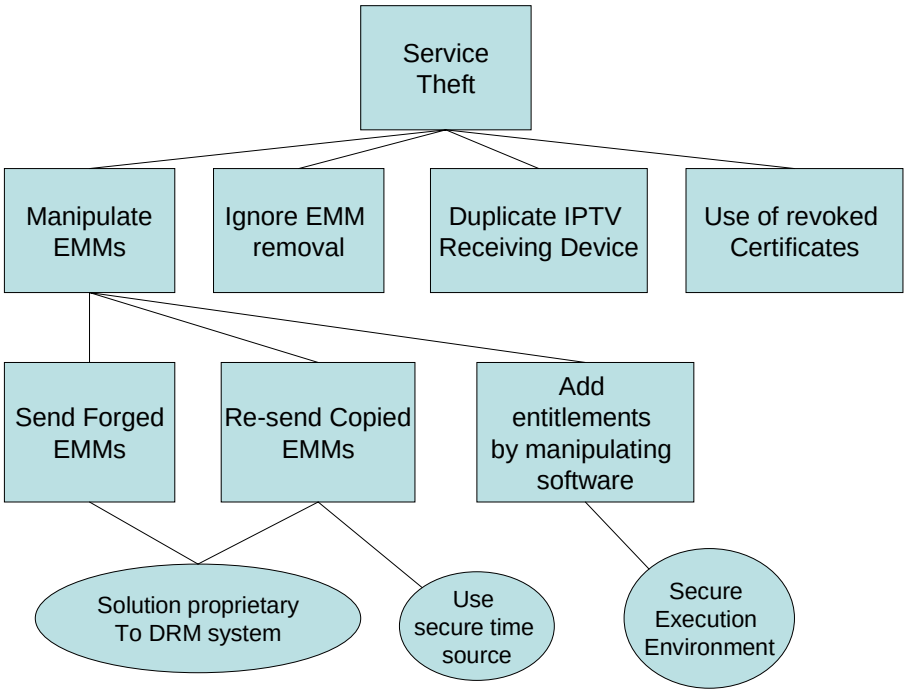


**Figure 9: IPTV Receiving Device - Service Theft - Manipulate EMMs - Attack Tree**

In the above attack tree, a single mitigation strategy may not be sufficiently robust, and multiple mitigation measures may be required.

The next figure shows the attack tree for service theft by failure to ignore EMM removal:

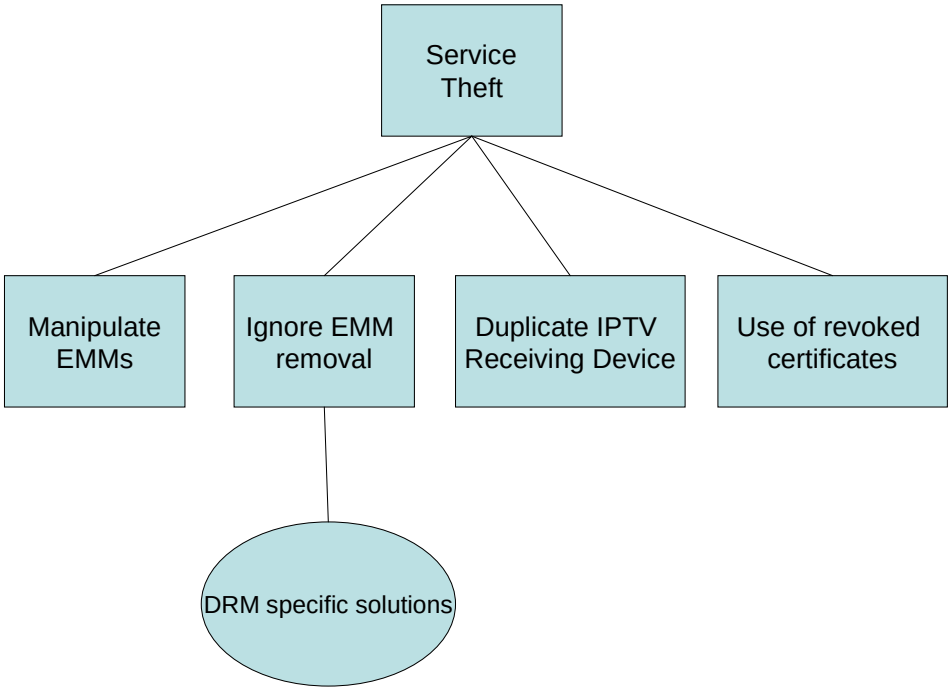


**Figure 10: IPTV Receiving Device - Service Theft - Ignore EMM removal - Attack Tree**

In the above attack tree, a single mitigation strategy may not be sufficiently robust and multiple mitigation measures may be required.

The next figure shows the attack tree for service theft by the presence of a duplicate IPTV Receiving Device:

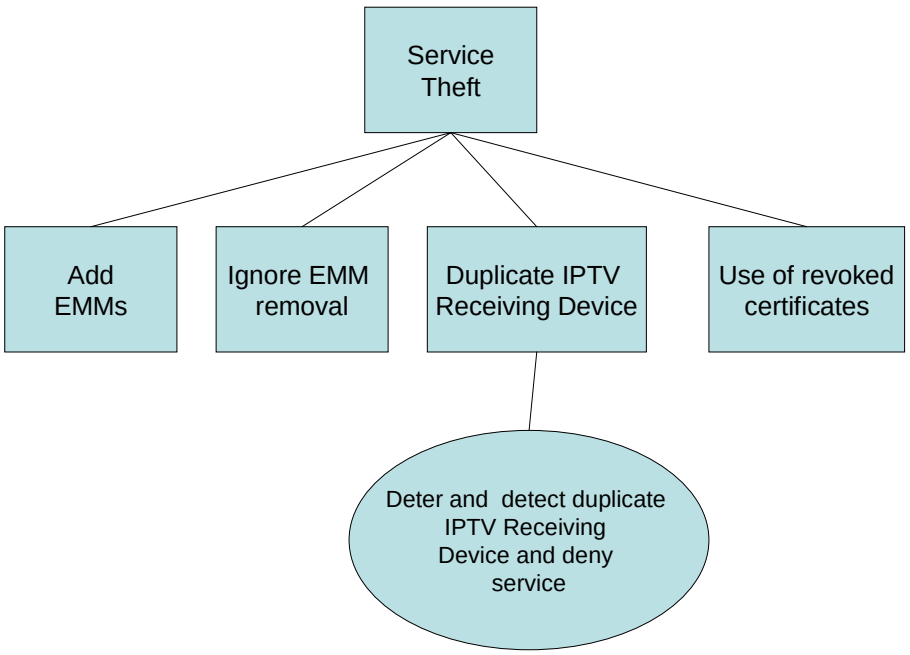


**Figure 11: IPTV Receiving Device - Service Theft - Duplicate Device - Attack Tree**

Part of the mitigation strategy of this vulnerability may also involve various levels of tamper proofing. Detection of duplicate devices can be very difficult for devices with one-way links. Detection would likely be possible only for 2-way devices.

#### 4.2.1.3 Information Theft

*Service* refers to initial delivery of content to IPTV Receiving Device. *Information theft* involves the acquisition of information about subscribers which the attacker is not entitled to. The next figure shows the information theft attack tree. This attack tree has four more sub-branches as shown:

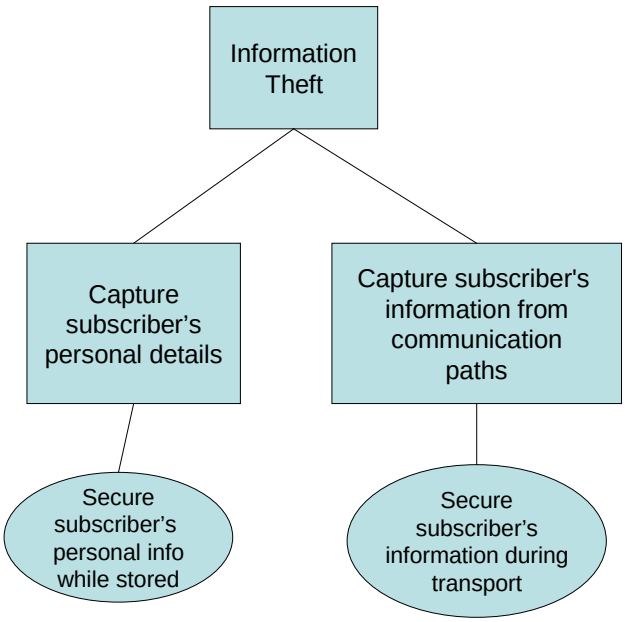


**Figure 12: IPTV Receiving Device - Information Theft - Attack Tree**

In the above attack tree, a single mitigation may not be sufficiently robust and multiple mitigation measures may be required.

#### 4.2.1.4 Service Disruption

*Service Disruption* involves either denying rightful access to services or making the experience poor. The next figure shows the attack tree for service disruption. This attack tree has three more sub-branches as shown.

##### 4.2.1.4.1 Rogue Network Disruption

Rogue network device sends offending code to headend, which sends code to all other devices and creates disruption of service. Mitigation is accomplished through authentication and secure execution of all downloads.

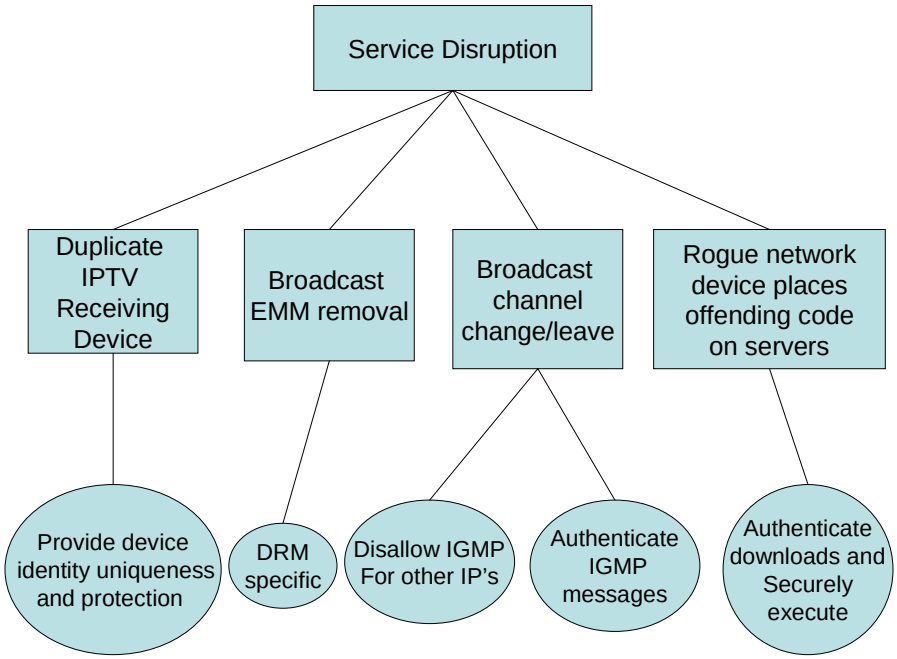


**Figure 13: IPTV Receiving Device - Service Disruption - Attack Tree**

This classic denial of service (DOS) attack is another vulnerability that must be mitigated. In the above attack tree, a single mitigation method may not be sufficiently robust and multiple mitigation measures may be required.

## *4.3 Threats to IPTV Devices*

### 4.3.1 Threats to Outputs and Paths

Decrypted IPTV content data *should not* be available on outputs other than those intended by the design of the IPTV Receiving Device (e.g., viewing screen). For devices that have multiple components that are connected via user-accessible connectors or buses, confidentiality protection needs to encompass such connections. In other words, confidential data such as DRM-related keys cannot be present on any user-accessible bus in unencrypted form, whether the data is in memory or in transit, including transit within the device. The definition of a user-accessible bus should be defined by a trust authority and is therefore out of the scope of this document.

### 4.3.2 Device Information Integrity

The identity of the IPTV Receiving Device, as defined at the time of manufacturing and recorded in device certificate, must be unique and protected from modification. This means the device identity in the certificate subject name is unique to the pool of all IPTV devices.

Although not a direct security robustness requirement, the identities included within ATIS device certificates and all other identities required for the network to authenticate, recognize, and authorize the device for ATIS-defined services must be unique. For instance, this could be accomplished by

establishing an IPTV Receiving Device identity naming convention in which the identity can be formed as a combination of a company- or organization-unique ID and a device-unique ID.

### *4.4 General Scope of Robustness Rules*

In order to address the threat analysis of the preceding sections, security robustness rules may be developed, and should consider, at the least, the following capabilities:

- Accurate identification of a valid IPTV Receiving Device.
- Tamper evidence and/or resistance.
- Protection of content in motion and at rest.
- Enforcement of content authorization.
- Security renewability.

## 5 DESIGN FOR INTEROPERABILITY

This section describes the IPTV Security Solution Interoperability Specification for the Security Robustness Rules.

### *5.1 Secure Execution Environment Elements*

The elements that comprise a SEE are as follows:

1) Execution Engine
2) Storage
3) Trusted Paths
4) Algorithms
5) Secure Time Generation
6) Physical Security

Any specific instance of a SEE will have a combination of different robustness levels of the above elements, and thus, this document specifies several levels of SEE robustness in section 5.2.

#### 5.1.1 Execution Engine

The execution engine is the computing element that performs the security functions embodied in the SEE.

#### 5.1.2 Storage

SEE storage consists of both the volatile and non-volatile memory used to implement the security functionality.

There are at least two ways to protect information while in this storage:

1) *Use hardware-based secure memory protection*, enabling the hardware to provide a proprietary method for memory protection without performing encryptions.

2) In the case of a lack of hardware-based secure memory protection, reliance can be made on a *unique, per-device secret that is protected by hardware* and is used to encrypt all the other values to be protected and then decrypt them when needed.

### 5.1.3 Trusted Paths

*Trusted paths* consist of all input and output ports from the SEE as well as all communication interfaces internal to the SEE.

### 5.1.4 Physical Security

*Physical security*, as defined in FIPS 140-2 [7], is the external indication that an attempt has been made to compromise a cryptographic module (i.e., the SEE) and possibly includes the capability of responding to that compromise attempt. In this document, physical security levels are described as follows:

- *Low Physical Security*: Having only the ability to show local evidence of tampering.
- *High Physical Security*: Having the ability to show local evidence of tampering and also to detect and respond locally to such tampering.

### 5.1.5 Algorithms

In compliance with the FIPS 140-2 concept of approved algorithms, this document uses the algorithms specified in the ISS/C, ISS/CA, ISS/R, ISS/A, ISS/E, and ISS/S toolkits as approved algorithms. Use of the approved algorithms qualifies as high robustness; use of any other algorithms qualifies as low robustness.

### 5.1.6 Secure Time Generation

*Secure time generation* refers to the process whereby a device supplies a secure time signal during the period between reception of consecutive network-secured time signals. Low and High security is based on the use of tools as defined in section 5.2.

## 5.2 Robustness Levels

When a SEE exists, this document defines two robustness levels (*Low* and *High*) for SEE elements which are related to the types of tools required to cause a breach. In addition, there is a classification for no robustness which pertains to cases when a SEE is absent.

### 5.2.1 No Element Robustness

Execution environments that can be compromised by the following tools are considered to have *no element robustness*, and thus are not considered secure.

- *Widely Available Tools*: General purpose tools or equipment that are widely available (such as screwdrivers, jumpers, clips, and soldering irons).

Note that this case is implied by ISS Security Profiles 0, 1, and 2 as defined in ATIS-0800014, *Secure Download and Messaging Interoperability Specification*.

### 5.2.2 Low Element Robustness

SEE elements that cannot be compromised by Widely Available Tools, but can only with great difficulty be compromised by the following tools have *low element robustness*:

- *Specialized Tools*: Specialized electronic tools or specialized software tools that are widely available, such as EEPROM readers and writers, debuggers, or de-compilers or similar software development tools.
    - However, Specialized Tools *exclude* Circumvention Devices – devices or technologies that are designed and made available for the specific purpose of bypassing or circumventing content protection.

### 5.2.3 High Element Robustness

SEE elements that cannot be compromised by Widely Available or Specialized Tools, but can only with great difficulty be compromised by the following tools, have *high element robustness*:

- *Professional Tools*: Professional tools or equipment that cannot be considered as Widely Available Tools or Specialized Tools, such as logic analyzers, chip disassembly systems, or in-circuit emulators.
    - However, Professional Tools *exclude* Circumvention Devices and tools or equipment that is made available only on the basis of a non-disclosure agreement.

## 5.3 Secure Execution Environment Levels

The following table gives the full scope of the defined SEE levels:

**Table 1: Secure Execution Environment Levels**

| SEE Level | SEE Element 1-5 Robustness | SEE Element 6 (Physical Security) Robustness |
|---|---|---|
| 0 | Low | Low |
| 1 | Low | High |
| 2 | High | Low |
| 3 | High | High |

The SEE has been defined based on the following elements: Execution Engine, Storage, Trusted Paths, Algorithms, Secure Time Generation, and Physical Security. Note that the only viable combinations for robustness levels of the first five SEE elements are all low or all high, so that a low robustness element does not compromise the high robustness features of another element. Physical Security, on the other hand, is understood to have a robustness level that is independent of the robustness level of the other five SEE elements.

## 5.4 Robustness Rules to FIPS 140-2 Mapping

The specification of the robustness for the SEE uses a subset of the FIPS 140-2 standard requirement. This document will consider only the FIPS elements listed in the table below.

A device that deploys a SEE must adhere to the following table of requirements for cryptographic modules at the designated FIPS 140-2 levels (specified in Table 1 of FIPS 140-2):

**Table 2: Robustness Rules to FIPS 140-2 Mapping**

| FIPS Requirement Name | FIPS 140-2 Level | Mapping to SEE Element Group | SEE Element Robustness Level |
|---|---|---|---|
| Cryptographic Boundary | – | 1-5 | SEE (includes, at least, security operating code, cryptographic key storage, and unique device identification materials). Low and High based on the use of tools as defined in section 5.2. |
| Approved Algorithms | – | 1-5 | ♦ *High* = Algorithms approved by IIF: (ISS/C, ISS/CA, ISS/R, ISS/A, ISS/E, and ISS/S)<br>♦ *Low* = All other algorithms. |
| Description of Cryptographic Module Software and Hardware | – | 1-5 | NSS (Manufacturer-specific), SEE |
| Ports and Interfaces | 3 | 1-5 | Encryption used to provide logical separation of cryptographic keys and critical security parameters from all other data, whether found on external data ports or internal communication links:<br>♦ *High* = ISS/E symmetric cryptographic algorithms (i.e., does not require use of ISS/E data structures).<br>♦ *Low* = All other algorithms. |
| Physical Security | 2 (Low), 3 (High) | 6 | SEE:<br>♦ *High* = Tamper Detection and Response.<br>♦ *Low* = Tamper Evidence Only. |
| Key Management | 3 | 1-5 | Low and High based on the use of tools as defined in section 5.2. |

NOTE -- Where the FIPS Level is designated as "–", the requirement is satisfied in the same way at all four FIPS levels.

NOTE -- The remaining FIPS 140-2 levels requirements that are not listed above are not required for qualification of the execution environment as a SEE. Specifically, for example, implementation of role based operator authentication, specification of finite state model, self test, design assurance, and multiple operator environments are not required. Specific self test-related software/firmware integrity-checking procedures are addressed in ATIS-08000014.

NOTE -- Column 4 of Table 2 defines the robustness criteria related to each of the FIPS 140-2 attributes that determine the level of robustness for the SEE elements. The following example illustrates this point:

When SEE level 2 (see Table 1) is chosen, SEE elements 1-5 must have robustness level "high" while SEE element 6 (physical security) can have robustness level "low". This means the FIPS attributes robustness levels would be as follows:

- Crypto boundary robustness level=SEE element 1-5, robustness level= high.
- Approved algorithm robustness level=SEE element 1-5, robustness level= high.
- Description of Cryptographic Module HW/SW: NSS, SEE.
- Ports and Interfaces robustness level=SEE element 1-5, robustness level= high.
- Physical security robustness level=SEE element 6, robustness level= low.
- Key management robustness level=SEE element 1-5, robustness level= high.

## 5.5 Confidentiality and Integrity Protection

IPTV Devices (including server-side and client-side) *shall* be designed and manufactured so as to provide confidentiality and integrity protection for the data types listed in the following table. The definition of the terms "confidentiality" and "integrity" are provided in section 3.1. Certain data types will also require Secure Storage.

**Table 3: Confidentiality and Integrity Protection**

| Data/Value | Confidentiality | Integrity |
|---|---|---|
| Device private key | Yes | Yes |
| Descrambling key | Yes | Yes |
| Device Information | No | Yes |
| Root certificate/s | No | Yes |
| Manufacturer DEV (sub-) CA certificate | No | Yes |
| Message Verification Certificate CA certificate | No | Yes |
| Management CA certificate | No | Yes |
| DRM component code | DRM-specific | DRM-specific |
| DRM component keys | DRM-specific | DRM-specific |
| Protected Content | DRM-specific | DRM-specific |
| Private User data (e.g., credit card info) | Yes | Yes |
| Secure Time Generation | No | Yes |

NOTE -- The confidentiality and integrity requirements placed on certain data/values are DRM-specific. Some values of this type are listed in this table for illustration purposes and are not covered by this specification.

The exact method of meeting these confidentiality and integrity protection requirements is out of scope of this document and is implementation-dependent.

## 5.6 Relationship to ISS Security Profiles

The sections below show the relationship of the ISS security profiles defined in ATIS-0800014 to the SEE and the robustness rules defined in this document.

### 5.6.1 ISS Profile Level 0

This profile does not require the existence of a secure execution environment; therefore, the robustness rules given in this document are not applicable.

### 5.6.2 ISS Profile Level 1

This profile does not require the existence of a secure execution environment; therefore, the robustness rules given in this document are not applicable.

### 5.6.3 ISS Profile Level 2

This profile does not require the existence of a secure execution environment; therefore, the robustness rules given in this document are not applicable.

### 5.6.4 ISS Profile Level 3

This profile does require the existence of a secure execution environment; therefore, the robustness rules given in this document are applicable.

In this profile, the ISS functionality is initiated with indirect authentication of its code or included certificates. However, since the software used in indirect authentication is required to run within the SEE, then its robustness is equivalent to the robustness of the SEE.

The SEE level, as defined in Table 4, serves as a sub-profile for ISS Profile Level 3.

**Table 4: SEE Sub-profiles of ISS Profile Level 3**

| SEE Level | ISS Profile – Sub-profile |
|---|---|
| Unspecified | 3 |
| 0 | 3-0 |
| 1 | 3-1 |
| 2 | 3-2 |
| 3 | 3-3 |

### 5.6.5 ISS Profile Level 4

This profile does require the existence of a secure execution environment; therefore, the robustness rules given in this document are applicable.

In this profile, the ISS functionality is initiated with direct authentication of its code or included certificates.

The SEE level, as defined in Table 5, serves as a sub-profile for ISS Profile Level 4.

**Table 5: SEE Sub-profiles of ISS Profile Level 4**

| SEE Level | ISS Profile - Sub-profile |
|---|---|
| Unspecified | 4 |
| 0 | 4-0 |
| 1 | 4-1 |
| 2 | 4-2 |
| 3 | 4-3 |

# 6 REQUIREMENTS TO SPECIFICATION MAPPING

This specification addresses, in whole or in part, the following requirements of ATIS-0800001.v002, *IPTV DRM Interoperability Requirements (Version 2)*.

**IIF.DRM. GENERAL.0400 –** For certain content types (such as movies that are stored on a PVR), the IPTV security solution *may* provide stronger cryptographic measures to protect against theft.

**IIF.DRM.General.0800-0200** - The IPTV Receiving Device DRM interface *shall* provide the capability to the IPTV Receiving Device DRM Component to exchange keys securely with other trusted hardware within the IPTV Receiving Device when the decryption is done by hardware other than what the IPTV Receiving Device DRM runs on.

**IIF.DRM.General.1800** - The IPTV Security Solution *shall* support physical tamper-resistance.

**IIF.DRM.General.1900** - The IPTV Security Solution *shall* support physical tamper-detection.

**IIF.DRM.General.2200** - The IPTV security solution *shall* provide a secure execution environment in the IPTV Receiving Device by supporting secure boot-loading and secure installs and updates of middleware and applications for the IPTV Receiving Device DRM Component.

**IIF.DRM.Operator.0300** - The IPTV Security Solution *shall* provide a mechanism to allow the TV operator to identify an IPTV Receiving Device DRM Component and its associated IPTV Receiving Devices.

# ANNEX A (INFORMATIVE)

## A.1 Requirements Labeling Guideline

The requirements will be labeled with textual tags of the following format:

CC[.TF].AAA.XXXXXX[-YYYYYY][-ZZZZZZ][-…..

- CC.[TF]is the top level notation that denotes the Committee (or Forum) and the TF (or Subcommittee) where standard was formulated. It may be an abbreviation or other semantics that are carried across the document. For this standard: IIF.DRM is used.
- AAA is a label identifying the requirement area. Usage of these mnemonic labels is determined on the project level. If the labels are used, they may have the format as suggested below. Other labels may be created as needed.
    - Operator
    - Subscriber
    - Interoperability
    - Scrambling
    - etc.
- XXXXXX is the parent numerical requirement tag. These numerical strings identifying individual requirements should not form a sequence of consecutive numbers. Adequate gaps should be left between individual requirement numbers to allow insertion of additional requirements in the future, if needed, without re-sequencing of the existing numbers.
- YYYYYY is the low level requirements numerical tag used to show that YYYYYY is a functional requirement that is a decomposition (or child) of DD.AAA.XXXXXX requirement. This parent child relationship can be extended to any level (e.g., ZZZZZZ). The "-"delimiting character in the label string indicates the parent-child relationship of the two requirements.

For example: **IIF.DRM.**Operator.0100 is a requirement for operator functionality. **IIF-DRM. Operator.0100-0100** would be a requirement that further defines (and is the child of) **IIF-DRM. Operator.0100**. **IIF-DRM.Operator.0100-0200** would be an additional requirement that further defines (and is the child of) **IIF-DRM.Operator.0100**.

Requirements tags will be in *italicized text***.**

The word "shall" will be understood as denoting a mandatory requirement. "Shall" will be used wherever the criterion for conformance with the specific recommendation requires that there be no deviation.

The word "should" shall denote a recommendation. "Should" shall to be used wherever noncompliance with the specific recommendation is permissible.

The words "conditional mandatory" shall denote a requirement the implementation of which is optional, but which if it is implemented shall be implemented in the exact manner specified. Conditional Mandatory statement will be bold in the document.

The word "may" shall denote a optional capability that may augment the standard. The standard is fully functional without the incorporation of this optional capability.